



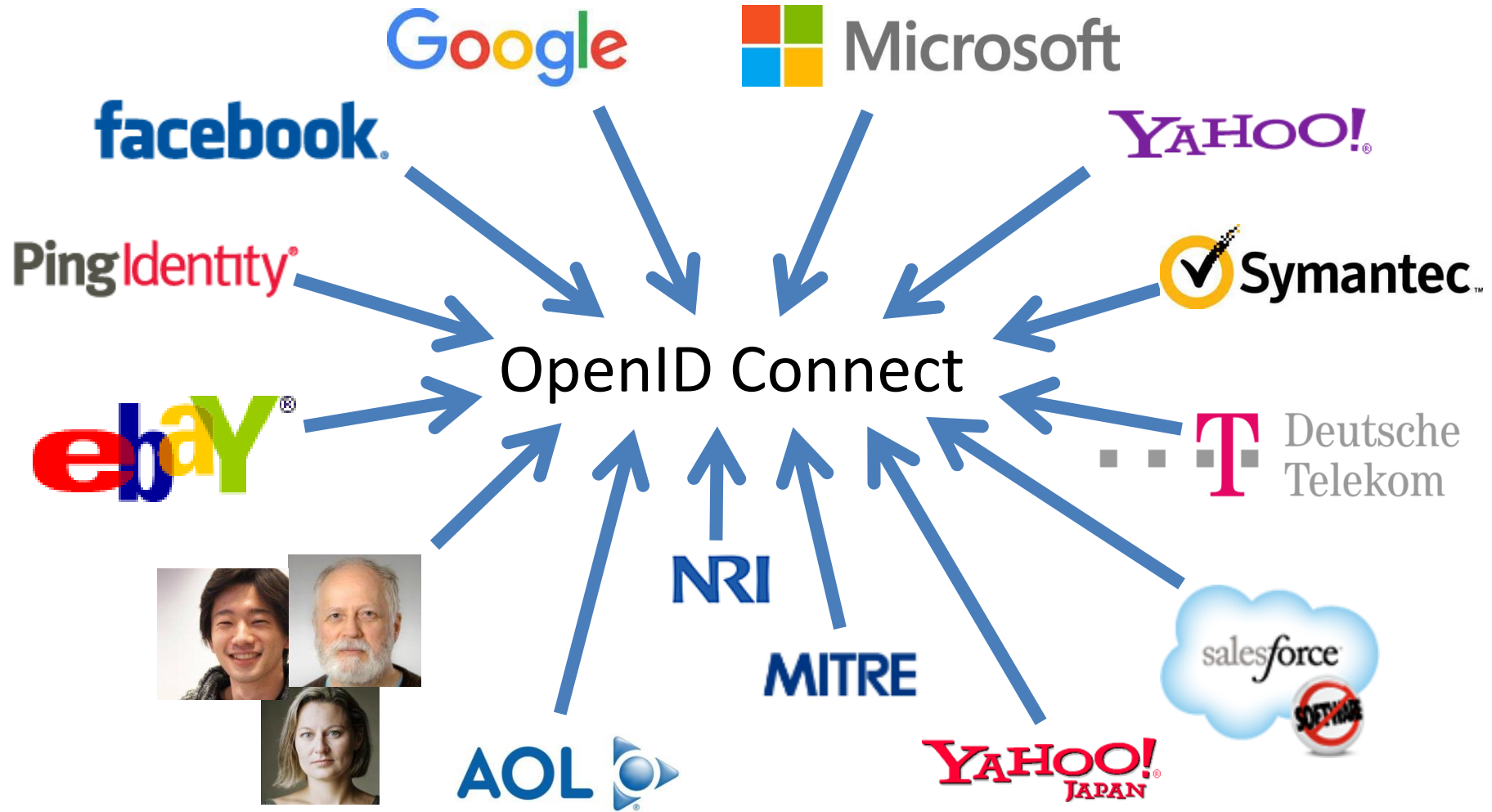
OpenID Connect Working Group

May 14, 2019

Dr. Michael B. Jones

Identity Standards Architect – Microsoft

Working Together



You're Probably Already Using OpenID Connect! OpenID

- If you have an Android phone or log in at AOL, Deutsche Telekom, Google, Microsoft, NEC, NTT, Salesforce, Softbank, Symantec, Verizon, or Yahoo! Japan, you're already using OpenID Connect
 - Many other sites and apps large and small also use OpenID Connect

What is OpenID Connect?



- Simple identity layer on top of OAuth 2.0
- Enables RPs to verify identity of end-user
- Enables RPs to obtain basic profile info
- REST/JSON interfaces → low barrier to entry
- Described at <https://openid.net/connect/>

OpenID Connect Range



- Spans use cases, scenarios
 - Internet, Enterprise, Mobile, Cloud
- Spans security & privacy requirements
 - From non-sensitive information to highly secure
- Spans sophistication of claims usage
 - From basic default claims to specific requested claims to collecting claims from multiple sources
- Maximizes simplicity of implementations
 - Uses existing IETF specs: OAuth 2.0, JWT, etc.
 - Lets you build only the pieces you need

Numerous Awards



- OpenID Connect won 2012 European Identity Award for Best Innovation/New Standard
 - <http://openid.net/2012/04/18/openid-connect-wins-2012-european-identity-and-cloud-award/>
- OAuth 2.0 won in 2013
- JWT/JOSE won in 2014
- OpenID Certification program won 2018 Identity Innovation Award and 2018 European Identity Award



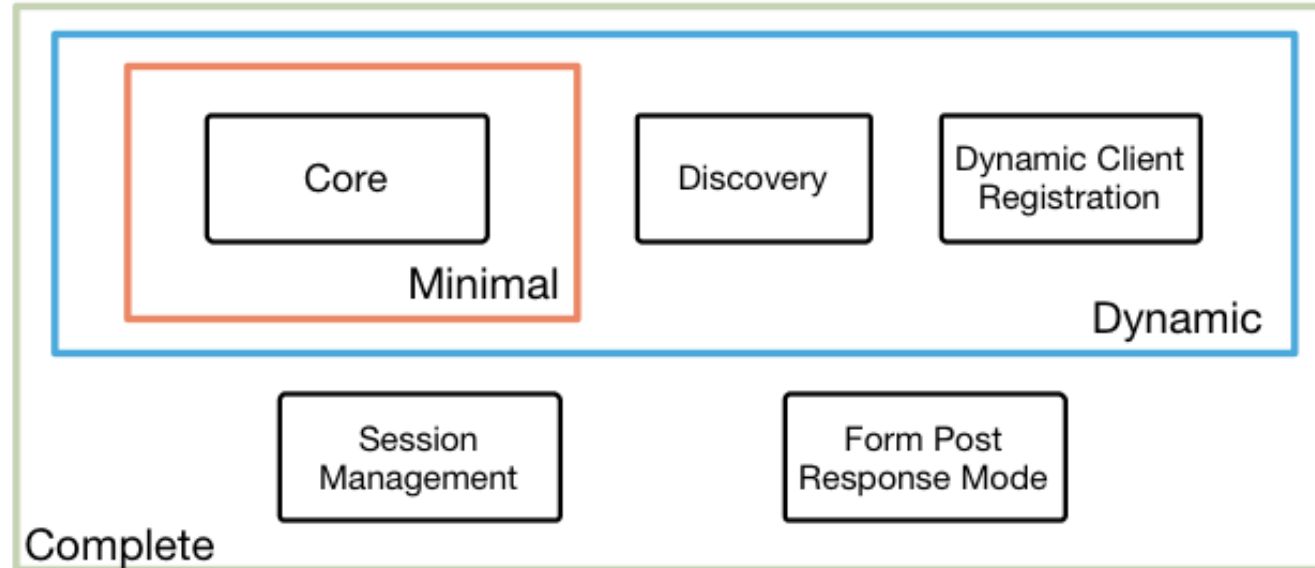
Original Overview of Specifications



4 Feb 2014

OpenID Connect Protocol Suite

<http://openid.net/connect>



Underpinnings



OAuth 2.0 Form Post Response Mode (additional Final Specification)



- Defines how to return OAuth 2.0 Authorization Response parameters (including OpenID Connect Authentication Response parameters) using HTML form values auto-submitted by the User Agent using HTTP POST
- A “form post” binding, like SAML and WS-Federation
 - An alternative to fragment encoding
- https://openid.net/specs/oauth-v2-form-post-response-mode-1_0.html
- Completed April 2015
- In production use by Microsoft, Ping Identity

OpenID 2.0 to OpenID Connect Migration (additional Final Specification)



- Defines how to migrate from OpenID 2.0 to OpenID Connect
 - Has OpenID Connect identity provider also return OpenID 2.0 identifier, enabling account migration
- https://openid.net/specs/openid-connect-migration-1_0.html
- Completed April 2015
- Google shut down OpenID 2.0 support in April 2015
- Yahoo, AOL, others also plan to replace OpenID 2.0 with OpenID Connect

Current Work



- Current OpenID Connect Specification Work:
 - Session Management / Logout
 - Federation Specification
 - Identity Assurance Specification
 - Native SSO Specification
 - Second Errata Set
- Related Working Groups
- OpenID Certification

Session Management / Logout



- Three approaches being pursued by the working group:
 - Session Management
 - https://openid.net/specs/openid-connect-session-1_0.html
 - Uses HTML5 postMessage to communicate state change messages between OP and RP iframes
 - Front-Channel Logout
 - https://openid.net/specs/openid-connect-frontchannel-1_0.html
 - Uses HTTP GET to load image or iframe, triggering logout
 - Similar to options in SAML, WS-Federation
 - Back-Channel Logout
 - https://openid.net/specs/openid-connect-backchannel-1_0.html
 - Server-to-communication not using the browser
 - Can be used by native applications, which have no active browser
- All support multiple logged in sessions from OP at RP
- Unfortunately, no one approach best for all use cases
- Certification tests being developed
 - WG plans to test multiple implementations before making specs Final

Federation Specification



- OpenID Connect Federation specification
 - https://openid.net/specs/openid-connect-federation-1_0.html
- Enables establishment and maintenance of multi-party federations using OpenID Connect
- Defines hierarchical JSON-based metadata structures for federation participants
- Implementer's Draft status reached
- Substantial changes since then
 - *Please review!*

Identity Assurance Specification



- OpenID Connect for Identity Assurance
 - <https://openid.net/specs/openid-connect-4-identity-assurance.html>
- Representation for verified person data
 - Enables legal compliance for some use cases
- New specification by Torsten Lodderstedt
 - *Please review!*

Native SSO Specification



- Enables Single Sign-On across apps by the same vendor
- Assigns a device secret issued by the AS
- New specification being written by George Fletcher
 - *Watch the WG mailing list for draft soon to come*

Second Errata Set



- Errata process corrects typos, etc. discovered
 - Makes no normative changes
- Edits under way for second errata set
- https://openid.net/specs/openid-connect-core-1_0-24.html is current Core errata draft

Related Working Groups



- International Government Profile (iGov) WG
 - Developing OpenID Connect profile for government & high-value commercial applications
- Enhanced Authentication Profile (EAP) WG
 - Enables Token Bound ID Tokens
 - Enables integration with FIDO and other phishing-resistant authentication solutions
- **Mobile Operator Discovery, Registration & authentication (MODRNA) WG**
 - Mobile operator profiles for OpenID Connect
- Financial-grade API (FAPI) WG
 - Enables secure API access to high-value services

OpenID Certification



- Enables OpenID Connect and FAPI implementations to be certified as meeting requirements of defined conformance profiles
- Now OP and RP Connect certification profiles for:
 - Basic OP and Basic RP
 - Implicit OP and Implicit RP
 - Hybrid OP and Hybrid RP
 - OP Publishing and RP Using Configuration Information
 - Dynamic OP and Dynamic RP
 - Form Post Response Mode for OP and RP
- FAPI OP certification launched April 1, 2019
- See <https://openid.net/certification/>
 - And accompanying certification presentation!



Open Conversation



- How are you using OpenID Connect?
- What would you like the working group to know and do?

OpenID Connect Resources



- OpenID Connect
 - <https://openid.net/connect/>
- Frequently Asked Questions
 - <https://openid.net/connect/faq/>
- Working Group Mailing List
 - <http://lists.openid.net/mailman/listinfo/openid-specs-ab>
- OpenID Certification Program
 - <https://openid.net/certification/>
- Certified OpenID Connect Implementations Featured for Developers
 - <https://openid.net/developers/certified/>
- Mike Jones' Blog
 - <http://self-issued.info/>
- Nat Sakimura's Blog
 - <http://nat.sakimura.org/>
- John Bradley's Blog
 - <http://www.thread-safe.com/>